

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

For each cell tower in described in Attachments A-1 through A-3, the cellular service providers identified in Attachments A-1 through A-3 are required to disclose to the United States records and other information (not including the contents of communications) about all communications or interactions made using the cellular tower(s) identified in Attachments A-1 through A-3 during the corresponding timeframe(s) listed in Attachments A-1 through A-3, including records that identify:

- a. the telephone call number and unique identifiers for each wireless device in the vicinity of the cell tower (the locally served wireless device) that registered with the cell tower, including Electronic Serial Numbers (ESN), Mobile Electronic Identity Numbers (MEIN), Mobile Identification Numbers (MIN), Subscriber Identity Modules (SIM), Mobile Subscriber Integrated Services Digital Network Numbers (MSISDN), International Mobile Subscriber Identifiers (IMSI), and International Mobile Equipment Identities (IMEI);
- b. for each communication or interaction, the “sector(s)” (i.e., the face(s) of the tower(s)) that received a radio signal from the locally served wireless device;
- c. the date, time, and duration of each communication or interaction;
- d. the source and destination telephone numbers associated with each communication or interaction (including the number of the locally served wireless device and the number of the telephone that transmitted a communication to, or to which a communication was transmitted by, the locally served wireless device);

- e. the type of the communication or interaction transmitted through the tower (such as phone call or text message); and
- f. all specialized location information including Timing Advance, RTT, LocDBoR, or similar.

These records should include records about communications or interactions that were initiated before or terminated after the timeframe(s) identified in Attachments A-1 through A-3 if some part of the communication or interaction occurred during the relevant timeframe(s) listed in Attachments A-1 through A-3.

II. Information to be Seized by the Government

Upon receiving the requested information from the Wireless Providers, the data will be provided to an independent investigative unit to be reviewed for completeness and scope. This unit will then review the raw data to identify devices likely associated with the criminal offenses under investigation based upon the totality of the characteristics of each device, which may include, but is not limited to:

- a. Devices that appear in the area of the relevant location at the at the appropriate dates and times;
- b. Devices whose records indicate that the device traveled to the area of the relevant location and/or departed from the area of the relevant location at times consistent with the known facts of the investigation;
- c. Devices that appear to be actively communicating with the cellular network versus devices that appear to be passively communicating with the cellular network;
- d. Devices that display usage characteristics consistent with the known facts of the investigation; and/or,

- e. Devices that are recorded to be located at distances from the surrounding cell sites consistent with the distance of the relevant location.

Following an independent analysis of the information from the Wireless Providers, the independent investigative unit will compile a report containing a list of devices determined to display characteristics consistent with the known facts of the investigation that may be associated with the offenses under investigation. This report, which will omit all devices determined to be unrelated to the investigation, will be provided to the investigative team for follow-up.

Law enforcement will make no affirmative use of information associated with devices determined to be unrelated to the offenses under investigation other than to identify those devices possibly associated with the subject of the investigation or possible witnesses of the criminal offense. After the review and analysis has been completed by the independent investigative unit, the raw files received from the Wireless Providers will be sealed and no longer accessed absent further order of the Court.